Study on Security Problems in WiMAX Technology

Daniel SIMION[1], Adrian GRAUR[2] and Alin Dan POTORAC[3]
"Stefan cel Mare" University
str.Universitatii nr.13, RO-720229 Suceava
Suceava, Romania

***Abstract*—Nowadays anyone from anywhere in the all world can access all types of data with a high level of QoS. The wireless industry continues to change day by day, tending to use the equipment more easily and safely and with a connection speed that tends to be higher and higher. But this mobility has its price. Intruders or illegitimate users can access important data and data is money. For this reason technologies used in data transmission need extra data security. Even if WiMAX technology has complex authentication and authorization methods and very strong encryption techniques is still vulnerable on different attacks or threats like jamming, scrambling or water torture attacks.**

This paperwork is an overview of most threats involved in infrastructure and WiMAX deployment and the security solutions needed to overcome them.

***Index Terms*—attacks, security, threats, WiMAX, wireless.**

I. INTRODUCTION

WiMAX is the abbreviation for ***W***orldwide ***I***nteroperability for ***M***icrowave ***A***ccess, and "Max" is used in order to express the very broad coverage provided by this standard. It is a new technology in the modern telecommunication and is used for high speed data transmission.

WiMAX is defined by the IEEE 802.16 standard and offers a set of technological improvements to wireless performance (throughput, coverage, indoor penetration). These improvements are: AMC (adaptive modulation and coding) which offers the highest available data rate based on link quality, sub channel division using SOFDMA (Scalable Orthogonal Frequency Division Multiple Access) – support bandwidths between 1.25 – 20 MHz, H-ARQ (Hybrid Automatic repeat Request), FEC (Forward Error Correction) and smart antennas that use MIMO and AAS (Adaptive Antenna System) [1].

Security threats are a problem that needs more research in order to find solutions to these threats, fact that will help WiMAX to become a successful and reliable technology. To exchange data with a higher protection between MAC and PHY layers, WiMAX has define a security sublayer on the ground of the MAC layer, which contains privacy and key management and protects the data communication from hijacking attacks between SS and BS. The PKM protocol represents the main protocol from security sublayer which provides authentication, key management and a better privacy for data traffic. Also, protection keys, like AK, TEK, KEK or HMAC, which are used in security sublayer, provide a better security for WiMAX technology. But security risks, threats or vulnerabilities are still available for WiMAX technology.

This paper was supported by the project "Knowledge provocation and development through doctoral research PRO-DOCT - Contract no. POSDRU/88/1.5/S/52946", project co-funded from European Social Fund through Sectoral Operational Program Human Resources 2007-2013.

II. WiMAX ARCHITECTURE

The WiMAX protocol architecture is structured into two major layers (see Figure 1): - the *MAC (Medium Access Control) layer* and the *PHY (Physical) layer.*

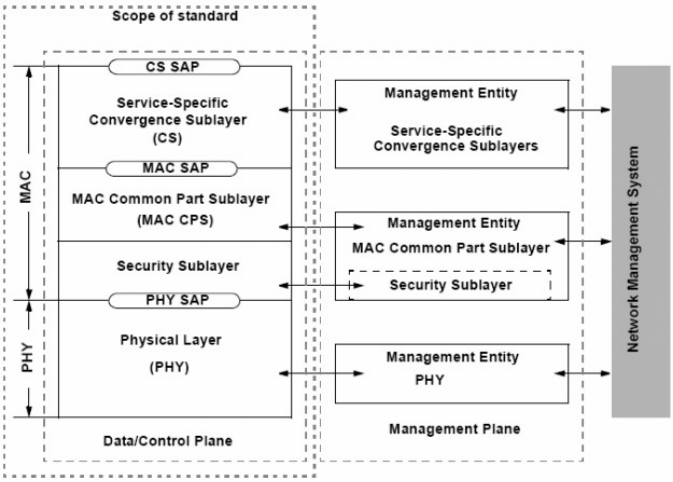

Fig. 1 WiMAX protocol layers [2]

MAC layer is composed of three sublayers. Starting from the base, the fist sublayer is SS (Security Sublayer) which encrypts and decrypts the data which are entering and leaving in and from PHY layer. This sublayer uses for data traffic 56bit DES encryption and for Key Exchanges uses 3DES encryption [3].

The second MAC sublayer is the CS (Service Specific

Convergence Sublayer). This sublayer maps higher level data services to MAC layer service flow and connections [4, 5].

The third sublayer is the CPS (Common Part Sublayer). In this sublayer are constructed the MAC PDUs. The CPS sublayer defines rules and mechanisms for ARQ (Automatic Repeat Request 10), for connection control and for system access bandwidth allocation. It also provides centralization, channel access and duplexing. CS and CAP are communicated by MAC SAP (Service Access Point) [3].

The *PHY layer* it's a bridge between MAC PDU and the physical layer frames, sent and received through modulation and encoding of RF signals.

Figure 2 shows the WiMAX network architecture, consists of *SS (Subscriber Station)* or the *MS (Mobile Station)*, the *ASN (Access Service Network)* and the *CSN (Connectivity Service Network)*. The first two are parts of *NAP (Network Access Provider)*, while the last is a part of *NSP (Network Service Provider)*.

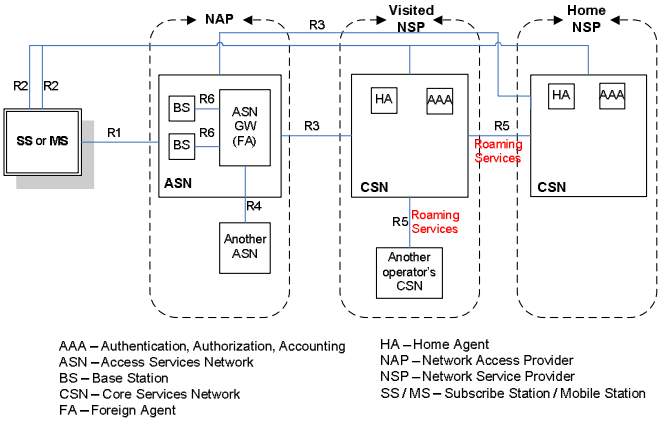

Fig.2 WiMAX Network Reference Model

WiMAX technology architecture was created so as to allow its connection with IP networks which provide Internet services (see Figure 3).

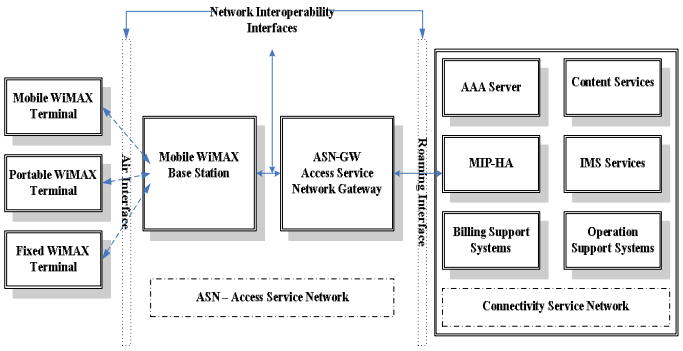

Fig. 3 WiMAX Network IP-Based Architecture [adapted after 1]

III. WiMAX Security Elements

The whole security mechanism of WiMAX technology is defined by SA (Security Association), X.509 certificates, PKM Authorization, Privacy and Key Management and Data Encryption.

A *Security Association* is composed from a set of security parameters which protects data and maintains the data transmissions at a certain level of safety. In the initialization phase, SS establishes the primary SA, which is unique per SS. Meanwhile, on the BS is configured the static SAs. During the dynamic transport connections, BS generates a dynamic SA and sends it to the SS. If the SS has more than one service flows, all dynamic SAs will be dynamically created and destroyed in real time while service flows are created and completed.

The BS makes sure that an SS access only the SA that is authorized to access it and respects the characteristics of that type of service which will be accessed by the SS. One SS can have one until three SAs, first being used for the secondary management channel and the second and/or the third being used for uplink and/or downlink channels. The downstream being protected by the primary SA, in multicast communication the primary SA can't protect it. For this reason are used static and/or dynamic SAs.

IEEE 802.16 standard supports 2 types of SAs – data and authorization SA. Data SAs protects the data transport connections between BS and SS and authorization SAs establishes the data SA and authorizes the SS to access the BS

An *Authorization SA* contains the following information [6]:

- X.509-Certificate – is a digital certificate used to identify the SS.
- Authorization Key (AK) – on 160-bit, is generated by the BS, is kept secretly between subscribe station and the base station and is used for generating Key Encryption Key (KEK).
- AK Sequence Number – contains 4 bits to identify the authorization key and it is serves for the differentiation between the successive AKs.
- AK-Lifetime (32Bits) – representing the validity duration of an AK. The AK Lifetime can be set between 1 – 70 days, but usually is set on 7 days.
- Key Encryption Key (KEK - 128Bits) – is used in BS to encrypt the Traffic Encryption Keys (TEKs) from a data SAs and to transmit it. For data encryption it is used Traffic Encryption Keys (TEKs). The SS will use later the KEK to decrypt the received encrypted TEKs.

A X.509 certificate is used for identification of SS. The standard doesn't define certificates for BS. A X.509 certificate defines an authentication algorithm based on public-key techniques. Each SS has a unique X.509 digital certificate which contains the SS's MAC address and the public key. The base station authenticates the subscribe stations when initial authorization exchange and in requesting time of an AK, SSs present to the BS the own digital certificate. Then, the BS checks them and used the public key for AK encryptions. Requesting SSs receive back

the AK and the BS associates for each SS an authentication identity, on which SSs are authorized to access, with the AK exchange, services like data, video or voice.

So, BS can avoid the cloned SSs attacks (***masquerades attacks***). SSs have RSA public/private key pairs installed at the factory or have an algorithm which generates dynamically RSA key pairs. In the second case, if the SS must generate its RSA key pair, this key pair will be generated before the AK exchanges.

For this reason SSs need to support a mechanism which installs the X.509 certificates issued by the manufacturer. Attackers must crack the encryption of the X.509 certificate used and must have an SS from the same manufacturer for succeeding his attacks on the BS, if the SSs have a factory-installed RSA private/public key pair.

In WiMAX, the security of connections access is accomplished by complying with the *Privacy Key Management protocol*. The utility of this protocol is that it provides periodical and normal authorization of SSs; it distributes keying material to them and also provides key refresh and reauthorization. Another task of PKM is to insure that the authentication algorithms and supported encryption are correctly applied to the exchanged MPDUs (MAC Protocol Data Units).

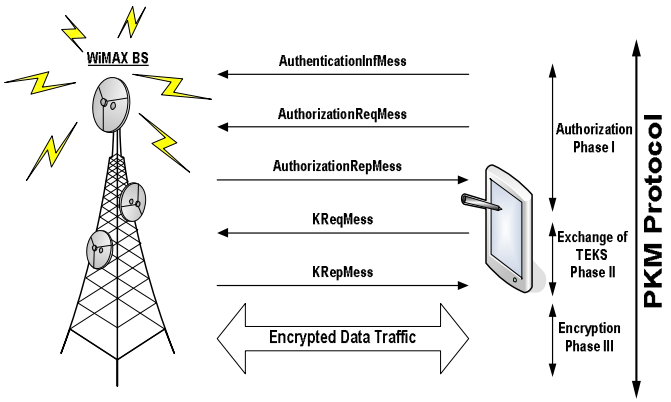

Fig. 4 Privacy Key Management Protocol Phases

In order to securely exchange keys between BS and SS, the PKM protocol uses the symmetric cryptography and X.509 certificates. As it is shown in Fig. 4, the protocol is based on three phases. The BS plays the role of the server and it manages the distribution of keying material to the SS, who plays the role of client. During the initial authorization exchange, when a BS authenticates a SS client, the PKM protocol is used. SS uses a digital certificate for authentication at the BS. Also, the PKM protocol uses public key cryptography for creating, between the BS and SS, a shared secret key. This is also used to allow periodic reauthorization and key refresh by the SS.

SS transmit an authentication message (*AuthenticationInfMess*) which contains the certificate of SS producer. In the same time, SS transmit another message which contains the authorization Request Message (*AuthorizationReqMess*) that request an AK (Authorization Key). The *AuthorizationReqMess* contains the SS's certificate; the cryptographic capabilities which contains a stack of cryptographic layers with a set of data authentication and encryption algorithms and the SAID (Security Association IDentifier) whose value is the same with the primary 16Bit CID (Connection IDentifier) that the BS sends it to the SS for the period of the initialization phase and the network entry. After that, the BS will verify the X.509 digital certificate; will choose the encryption algorithm and then will send the authentication response. Finally, the BS sends the RSA-public key encrypted AK to the requesting SS.

This process of authentication and key exchange between SS and BS, the first step of the PKM, is presented in the Fig. 5.

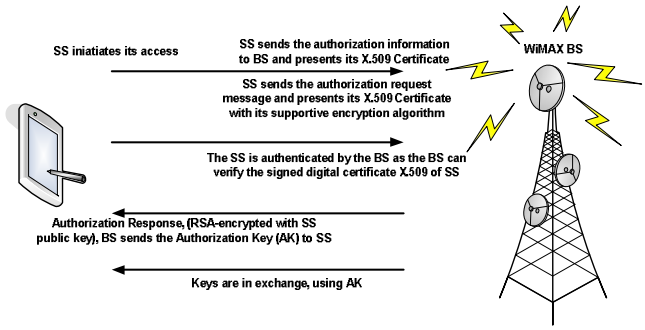

Fig. 5 Authentication and Authorization Key allocation by the BS [adapted after 7]

The next step of the PKM protocol is to initiate the exchange of TEKs and to establish a data SA (see Fig. 6).

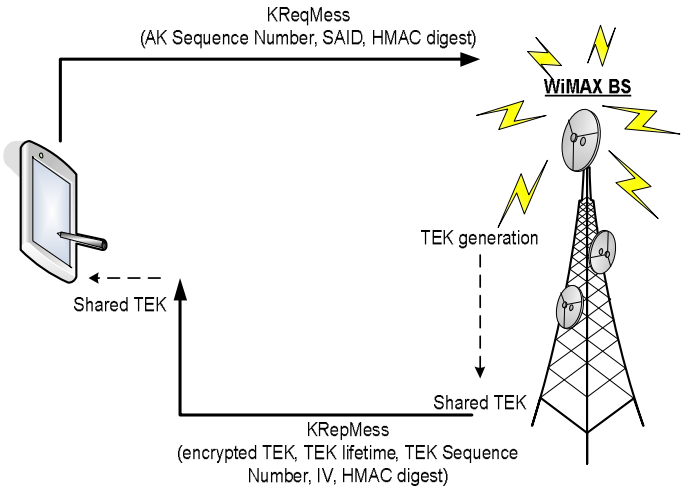

Fig. 6 TEKs exchange

Every SS sends regularly a Key Request Message (KReqMess) to the BS, asking it for the renewal of the TEK. If the received SAID matches the SA at the SS and after verifying the KReqMess message authenticity and the integrity by checking the HMAC digest, the BS will respond to that message. Then will also send a key Reply Message

(KRepMess) that contains the new key material needed by the TEK state machine. The BS keeps two active key materials per SAID at any time, and these are denoted by the TEK-Parameters in the KRepMess message.

The KRepMess message is composed of an AK sequence number, the SAID, the parameters linked to the old TEK, and the new TEK and an HMAC digest - in order to ensure the SS that the message is being sent by the BS without being tampered with. It is known that the validity durations of the two TEKs overlap. The new TEK is being activated before the old TEK expires, and the old TEK is destroyed after ensuring that the new TEK was activated.

In order to estimate when the BS will invalidate a previous TEK or request a new TEK, the SS uses the lifetime of a TEK. The BS will reply with a Key Reject Message which contains the AK sequence number, the SAID and an error code with an indication regarding the reason of rejection and a HMAC digest. The SS could thus resend a different KReqMess message to obtain a new TEK if the SAID in the KReqMess message is invalid.

The present described phase of the PKM protocol may well start by an optional message, denoted by RkeyMess. This precedes the KReqMess message. This message is sent by the BS to trigger rekeying before the SS requests it. It contains the AK sequence number, the digest of the message produced by the downlink HMAC key, and the SAID related to the SA whose keying materials are requested.

The third phase of Privacy Key Management Protocol is *Data Encryption* phase. The transmitted data between the SS and BS begins to be encrypted using the TEK only after achieving the SA authorization and the TEK trade.

Therefore, in IEEE 802.16, it is obtained two-tier key systems. First the PKM protocol authenticates an SS to BS when a shared secret key (AK) is established by public key cryptography and then the SS acquires the registration to the network when AK is used to secure the exchange of Traffic Encryption Keys (TEKs) [8].

At first, the BS creates two TEKS for each of SA. When the old one expires, it generates a new key. Among the two keys, the BS uses the older one to encrypt the downlink traffic. The two keys - depending on which key is being used by the SS - can be used for decrypting the uplink traffic.

Figure 7 illustrates a SS request to the BS for TEK0 and TEK1 encryption keys. The BS changes its key every time is expiring. The SS uses the newer of the two keys for encrypting the uplink traffic. On the other hand, for the downlink traffic, can be used either of the two keys - depending upon which key is used by the BS at that moment.

It is known that the TEKs have a limited lifetime and have to refresh regularly. The BS can use the newer TEK for encryption when the older TEK expires. It is the duty of the SS to bring up to date its keys periodically. A KEK is used by the BS in order to encrypt the TEK in the Key Reply (PKM-RSP) MAC management message.

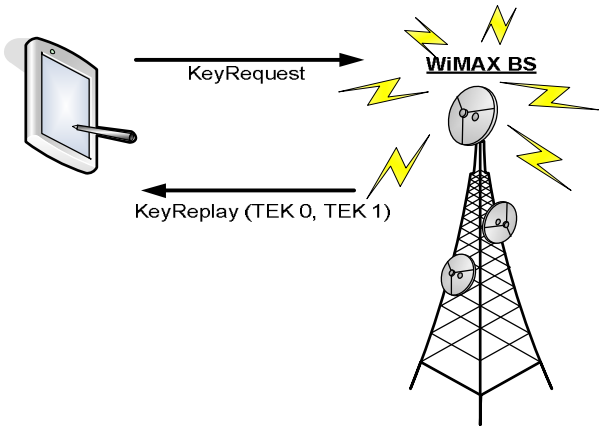

Fig. 7 SS sends a request to the BS for TEK0 and TEK1 encryption keys

The TEK can be encrypted using one of the following algorithms, using the KEK: 3-DES, RSA or AES. The TEK encryption algorithm is specified by the TEK encryption algorithm identifier in the cryptographic suite of the SA.

IV. WiMAX Security Threats

Security algorithm of WiMAX technology is implemented in the security sub layer, at the bottom of MAX layer and above to the PHY layer.

Thus, the PHY layer it's an open door for the hackers. IEEE 802.16 is vulnerable at the attacks like *jamming, scrambling or water torture attack*, most of all that supports mobility.

Like Michel Barbeau says in [9], a jamming attack is an attack *achieved by introducing a source of noise strong enough to significantly reduce the capacity of the channel*. A jamming attack can be easily launched, deliberately or undeliberately, with some equipments (radio spectrum monitor, for example), which are easy to obtain. In [10] are describe, step by step, techniques for this kind of attack.

Scrambling attacks are a kind of jamming attacks, except that these are for a short period of time and are directed to the PHY Layer, to certain WiMAX frames or some parts of them.

This type of attacks is a dangerous one and very difficult to be detected. Hackers focus them attacks to a definite connection, but in the same time they don't affects other users. Attackers can totally block one connection and at the same time and retransmission. Control message encryption can't ban very easy this threat. After the SA establishment, a control message is not encrypted, the only protection being offered by the CMAC/HMAC. So, the attackers can very easy manage the WiMAX CID (Control Message Information). CID assignment contains the user's connection CID. In that way, the attackers would know the information about the victim area connection, from the Medium Access Protocol (MAP) announced by BS allocation.

The hackers must know the MSID (Mobile Station IDentity)/NAI (Network Access Identity) of the victim-user, the services which are used by the victim and must hold radio

equipment which has a transmission range that can cover the victim-user and which can be able to send interference signals with the assigned frequencies. In the same time, hackers must synchronize with the MAP lifetime, because if they don't, all users of the same BS will be affected and the scrambling attack will be compromised.

A scrambling attack is presented in Fig.8.

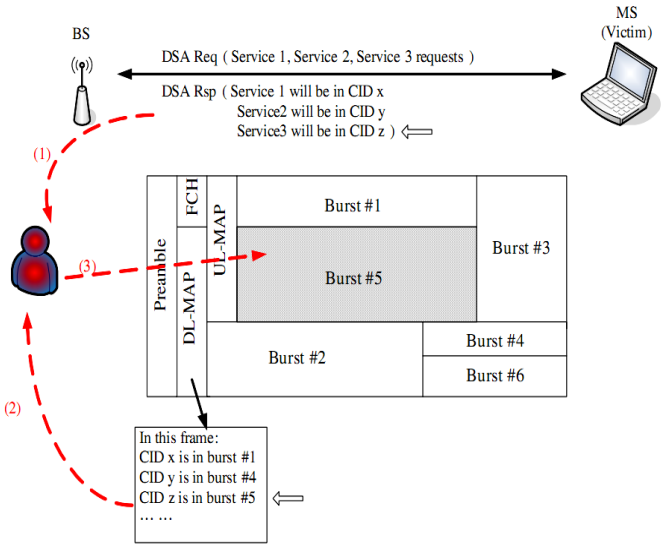

Fig. 8 Scrambling attack procedure [taken from 11]

In this scenario attackers wish to scramble the service 3. First of all, he must sniff the DSA (Digital Signature Algorithm) message and then the MAP information. With this information, the attackers know from the frame the target data region and can send interference signals.

Another threat in WiMAX wireless networks is when the attacker sends a series of frames to consume the receiver's battery; this kind of attack is called *Water Torture* (see Fig. 9).

Like most wireless networks, the signal may be high jacked using a RF receiver so a measure to prevent this type of behaviour is required (maybe a cryptographic security mechanism which can be maintained while a mobile Subscribed Station (SS) changes between WiMAX BS).

Data authenticity technology is required in order to prevent an attacker with a RF sniffer to capture, change and retransmit data frames to the WiMAX BS. When the transmission range is longer, a detection mechanism for relayed frames is needed to prevent attackers to forward data frames, from authorized stations that can't communicate directly.

Other threats in IEEE 802.16 standard are - *forgery attacks* - an attacker with an adequate radio transmitter can write to a wireless channel [12] and *replay attacks* – an attacker resend legitimate frames that he was intercepted its in the relaying process (or middle of forwarding).

The WiMAX security solutions at the MAC layer provide also a lot of defects or flaws.

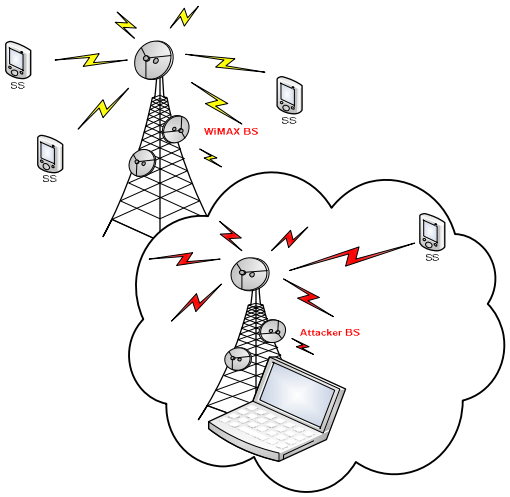

Fig. 9 Attacker BS uses Water Torture to create DoS attack

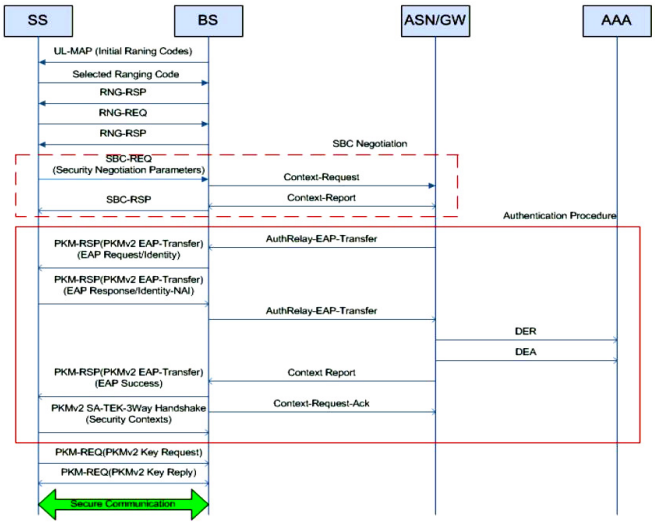

Fig. 10 An overview of the Initial Network Entry Procedure [taken from 15]

The Initial Network Entry procedure (see figure 10) it is the first gate to set up a connection to Mobile WiMAX by executing several actions like initial Ranging process, SS Basic Capability (SSBC) negotiation, PKM authentication and registration process. The initial network entry procedure has therefore a significant role in all processes. Using *Ranging Request-Response* (RNG-REQ, RNG-RSP) messages can be a difficult and vulnerable process because this message is used in the initial ranging procedure. When the SS is trying to connect to the network to suggest a request for burst profile information transmission, frequency, power and timing, a RNG-REQ message is also sent. After this, the BS responds by transferring a RNG-RSP message in order to fine-tune the setting of transmission link. If we want the uplink and downlink channel of the SS to change its state, we can use the RNG-RSP message.

There are few risks related to these types of messages. For instance, a certain attacker can intercept the RNG-REQ and change the most preferred burst profile of SS to the least effective one, thus downgrading the service [13, 14]. This

attacker can also spoof or change ranging messages in order to attack or suspend regular network activities and affect their performances. This vulnerability presented above can lead to a DoS attack.

Next, are presented other initial network entry vulnerabilities: - Taeshik Shon (and the others) presented a more general vulnerability of initial network entry in [15]: many important physical parameters and performance factors, security contexts between SS and BS, specifically the PKM security contexts and SBS negotiation parameters. Even if the security schemes offered WiMAX incorporate a message authentication scheme by utilising the HMAC/CMAC codes and traffic encryption scheme with AES based on PKMv2, these methods are applied only to normal data traffic after initial network entry process. The parameters exchanged during this process are not securely protected. This can bring a possible exposure to malicious users to attack.

In paper [15], Taeshik Shon (and the others), also presented a solution to this vulnerability, using Diffie-Hellman key agreement scheme, as shown in Figure 11.

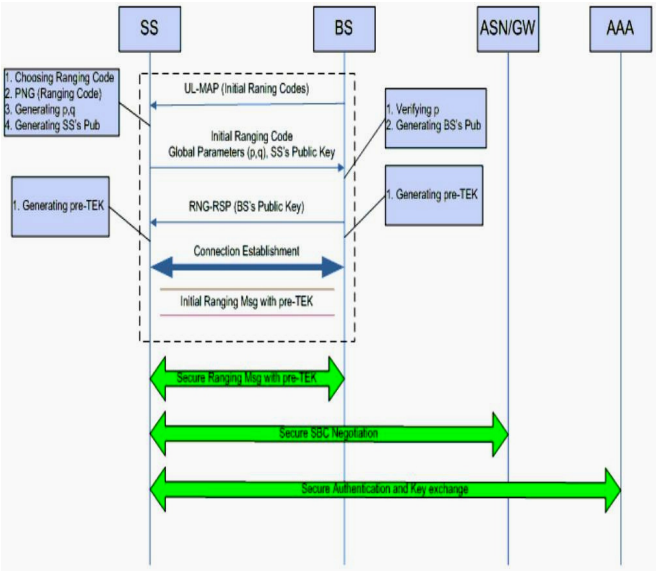

Fig. 11 The Taeshik Shon proposed Network Initial Entry [taken from 15]

In order, for the SS and BS, to produce a shared common key called pre-TEK separately and create a secret communication channels in the initial ranging procedure, a Diffie-Hellman key agreement scheme will be used. The SBC security parameters and PKM security contexts can be then exchanged securely.

Also, in [15], is reviewed the vulnerability in *ASN (Access Network Security)* of the WiMAX technology. In order to accommodate the requirements of WiMAX End-to-End Network Systems Architecture for mobile WiMAX network, the WiMAX forum defined NRM (Network Reference Model). This consists of the following entities: SS (Subscriber Station), ASN (Access Service Network) and CSN (Connectivity Service Network). The ASN is composed of at least one BS and one ASN Gateway (ASN-GW), forming a complete set of network functions that are necessary to give radio access to all mobile subscribers.

CSN is composed of AAA (Authentication, Authorization and Accounting) Proxy Server, Billing, Policy and Roaming Entities, and represents a complete set of network functions that provide IP connectivity services to subscribers. This AAA-architecture based model is depicted in the following figure.

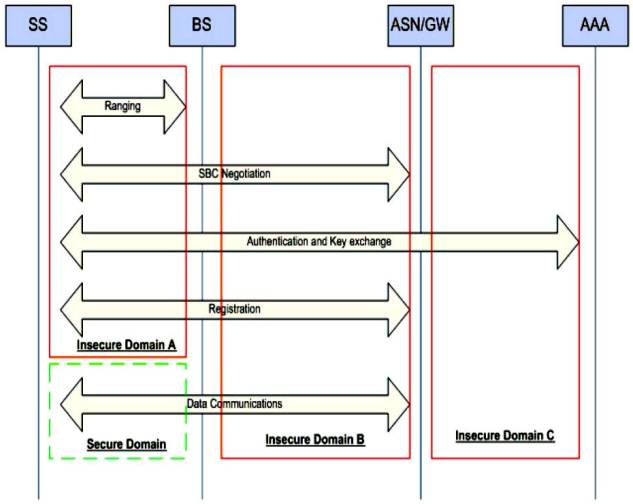

Fig. 12 An ASN Overview

Taeshik Shon and Wook Choi divided, also in paper [15], the model into one secure domain and other 3 insecure domains. The data communications between SS and BS is the only secure domain covered by encryption and authentication schemes in IEEE 802.16 standard. The initial network entry is related to domain A. Domain B and C are considered insecure because the Network Working Group in WiMAX forum believe that domain B is in a trusted network without proposing any security and just suggests a possibility for applying an IPSec tunnelling protocols between ASN and AAA in domain C.

A possible solution for this matter is represented by using a simple and efficient key exchange method based on PKI. Figure 13 presents this solution.

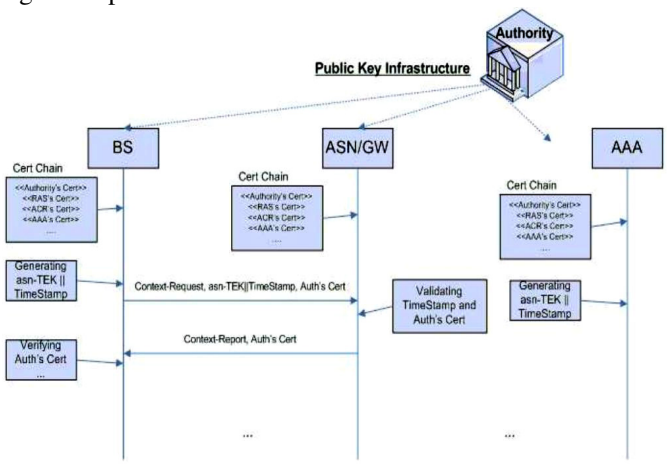

Fig. 13 Taeshik Shon's and Wook Choi's proposed ASN approach [taken from 15]

In this analysis, all network devices have a certificate chain for verification and their certificate. The PKI structure is used to achieve correspondent's public keys and validate the certificates, and it is also a method for enabling entities to generate a shared secret key for establishing a secure connection.

Serious threats arise from the WiMAX authentication scheme. In this context *masquerading* and *attacks on PKM authentication protocol* are the most significant. The masquerading problem consists of assuming, by a system, identity of another one. A masquerade attack possible can be made by means of sniffing and spoofing. There are two techniques to execute this type of attack:

- identity theft – is the case when a device is programmed with the hardware address of another device. This address can be stolen through interference of the management messages;

- rogue BS attack – in this case a false BS imitates a valid one, case in which all the SSs of that BS are compromised. The false (rogue) BS makes the SSs believing that they are connected to the legitimate BS, and then it can intercept the entire SSs' information. Because of the lack of mutual authentication, a MITM attack (Man-in-the-Middle-Attack) can be performed with a fake BS by sniffing messages related to authentication from the SS. In any situation it is quite difficult to successfully achieve this type of attack in WiMAX which supports mutual authentication by using PKMv2.

Bellow are presented some types of *attacks on the authentication protocols of basic PKM in IEEE 802.16 standard and its later version, PKMv2*.

Adopting the new version of PKM, WiMAX technology can fix a lot of flaws in PKMv1 such as susceptibility to MITM due to the lack of mutual authentication. Therefore, the newly proposed PKMv2 has been found to be also susceptible to new attacks [12].

In the PKMv1 attacks the messages can be intercepted and saved by the attacker of SS and then can execute a replay attack against the BS. The SS also might deal with this type of attack. Since mutual authentication is not supported in the basic PKM, BS is not authenticated. For that reason, malicious BS can perform a MITM attack, making its own Auth-Reply message and receives control of the communication of victim SS. Having many flows, the PKMv1 doesn't provide guarantees about the AKs (Authorization Keys) of SSs. These threats were fixed in the Intel Nonce version of PKM.

In Intel Nonce PKM version, nonce is a potential substitute for timestamp in authentication protocol. But, this method doesn't offer protection for a BS from a replay attack.

PKMv2 gives three-way authentication methods with a authorization message from SS to BS. The first attack on PKMv2 can be a replay attack which can be carried out if there is no signature by SS. On the other hand, even if the signature forms SS exists, an interleaving attack is still likely.

Some severe attacks can utilize vulnerabilities in many ways the MAC layers of IEEE 802.16 standard. The most important and critical attacks can be the *DoS* and *MITM attacks*. Even if WiMAX can prevent MITM attack throughout rogue BS using PKMv2, it is still susceptible to MITM molest. This opportunity is due to the vulnerabilities on the initial network entry. IEEE 802.16 standard doesn't supply any safety mechanism for the SSBC (Subscribe Station Basic Capability) negotiation factors.

In [16], is presented that in the SSBC negotiation procedure, through capturing and intercepting messages, attackers can imitate a valid SS and send modified SSBC response messages to the BS, when the communication between SS and BS is interrupted. The spy message would notify the BS that the SS hasn't security capability or supports few security capabilities. The communication between the SS and the BS won't have a powerful protection in the case that the BS still accepts. So, the attackers can eavesdrop and modify all the information transmitted.

A possible solution for this kind of attack is described in [16], where Tao Han (and the others) proposed SINEP (Secure Initial Network Entry Protocol). The SINEP solution is based on DH (Diffie-Hellman) key exchange protocol and enhances the security level throughout network initial. Approximately the same solution is offered in paper [15].

There are a lot of vulnerabilities which unveil mobile WiMAX networks to Denial of Services attacks (like - Reset-Command message, weak key sharing mechanism (in multicast and broadcast operations), undefended network entry, unencrypted management communication and unprotected management frame).

Denial of Service (DoS) attack is one of the most powerful on a wireless communication network. Using a two phased model service flow can be established. First is admitted a service flow with provisioned resources after which the service flow is activated on an on-demand basis. To conserve network resources the service flow can be activated or turned off after a certain time limit.

When a WiMAX network is either in Idle/Sleep Mode, with no uplink or downlink, the power consumption of the mobile station is lowered. Once the data is available, the base station establishes a connection with the mobile station using ranging parameters; ranging parameters that will be adjusted for the connection. In the end the mobile station returns to normal state with the activation of the service flow that permits data transfer. In some cases the mobile station will perform a series of operations to authenticate, to manage keys, to negotiate, to register and to re-establish IP connectivity. So, attackers may lunch different signaling attacks to the WiMAX base station to overload it with state transitions operations resulting in a denial of service attack [11].

Some of the most significant DoS attacks are:

- ✓ DoS attacks based on *RNG-REG/RNG-RSP* (Ranging Request/Response) messages: - when a RNG-RSP

message is created for minimizing the power level of a SS and making transmission very difficult to BS, thus activating frequently the initial ranging procedure. Also, an attacker can maximize the power level of SS and thus activating a *water torture attack*.

- ✓ DoS attacks based on MOB_NBR_ADV (Mobile Neighbour Advertisement) message: - in this case the serving base station sends MOB_NBR_ADV message to the SS with the characteristic of the BS that surrounds it. Because the message is not authenticated, this can be faked by attackers and in this way legitimate users can be deprived of services or, in the happy case, their services may have lower performance.
- ✓ DoS attacks based on FPC (Fast Power Control) message: - BS transmits a FPC message to the SSs that requires changing of its transmission power. This kind of message, also being of the management messages, which are not protected, can be easily intercepted and the attacker can use FPC message to avoid a SS from acceptably adjusting transmission power and communicating with the BS, and also can launch a water torture attack.
- ✓ DoS attacks based on *Auth-Invalid* (Authorization-invalid) message: - when an AK shared between BS and SS expired or when the BS is incapable to authenticate correctly the HMAC/CMAC, BS sends an *Auth-Invalid* message to SS. HMAC doesn't protect this message and in this way attackers can block SSs to use the network.
- ✓ DoS attacks based on *RES-CMD* (Reset-Command) message: - a BS can send a *RES-CMD* message in order to reset a SS that is malfunctioning or doesn't respond to commands, this message can also be used to initiate DoS attacks even if it is protected by HMAC.

The vulnerabilities in the initial network entry should be fixed in order to prevent DoS attacks and solution is that the authentication methods should be extended to as many as management frames as possible. For even a greater security, digital signatures can be used as an authentication method.

V. Solutions for Security Problems in WiMAX Networks

WiMAX standard has two types of certificates, one for SS and one for the manufacturer, and not for BS. This becomes a problem. Subscriber certificate identifies a subscriber by its MAC address. SS certificates are normally created and signed by the manufacturer using public key, this enables the BS to validate a SS certificate and so identify a certain device as genuine. This type of drawback is called *mutual authentication* problem.

Creating a scheme for mutual authentication is the only way that attackers can't forger or replay attack on a BS, for example with X.509 certificate you can verify EAP encryption [28]. A defense shield for the *man-in-the middle attacks* or the *forgery attacks* is made by PKM-MSH protocol, which ensures the mutual authentication.

A possible solution for the *jamming attack* was described in [9]. Increasing the power or the bandwidth of signals using techniques like FHSS (Frequency-Hopping Spread Spectrum) or DSSS (Direct-Sequence Spread Spectrum) it can avoid the jamming attacks. Also, with a radio monitoring equipment jamming attacks could be detected and compromised.

The attacks on the DES-CBC encryption algorithm can be avoided by using a randomly generated initialization vector (IV) placed in the payload, instead of the current one that is predictable and the attackers are able to get it. In this way, data won't be decrypted and the attackers won't predict the initialization vector.

To prevent a *water torture attack*, is essential a sophisticated mechanism to reject the false frames. To prevent *forgery and replay attacks* presented above it must be used mutual authentication.

Also, for the most powerful attacks, *scrambling attacks*, a possible solution, called DCJS (Dynamic CID Jumping Scheme) based on a key-dependent one way function and the DH (Diffie-Hellman) protocol is presented in [11], by Po-Wen Chi.

Figure 14 presents a MS entry procedure in DCJS. MSi has only two transport connections: - first is for uplink and the second is for downlink. CB, CU, CD and CP, correspond to the basic, the uplink and to the downlink CID and to the primary CID. In the index is represented the order in the same connection. In the left is described the CID used in transmission. In first step, using Diffie-Hellman algorithm, MSi and BSj establish an initial jumping key KI. After the PKM procedure, the jumping will change to KT assigned by BSj.

An essential improvement on WiMAX security mechanism is to add the CertificateChainRequest and CertificateChainReply messages for enabling a node which will verify the AuthorizationsNodeCertificate where the messages complete the RSA authentication within the PKM-MSH.

The IEEE 802.16 standard has improved mutual authentication between BS and SS where random numbers are included to stop replay attacks. In order for the handshake identification to be successfully fallowed the RSA based authentication has incorporated its own certificate. The handshake identification is done following the next steps [17]:

1) RSA-Request (SS →BS): MS_Random, MS_Certificate, SAID, SigSS.

2) RSA-Reply (SS →BS): MS_Random, BS_Random, Encrypted pre-PAK, Key Lifetime, Key Sequence Number, Bs_Certificate, SigBS

3) RSA-Acknowledgement (SS →BS): BS_Random, Auth Result Code, Error-Code, Display-String, SigSS.

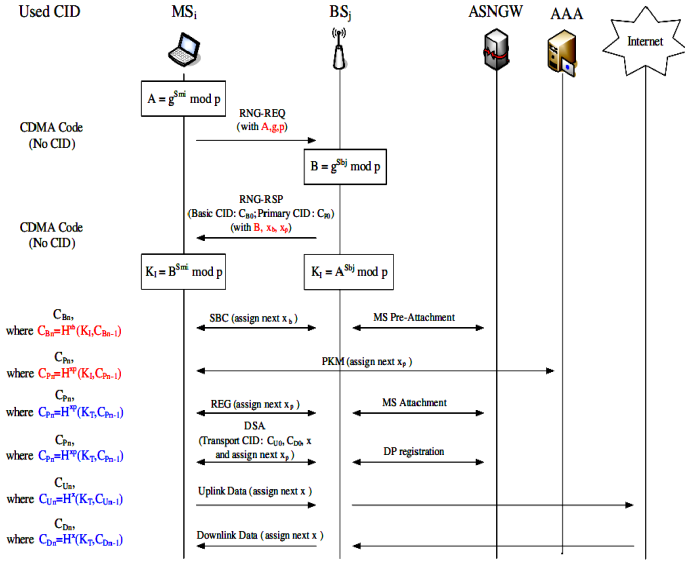

Fig. 14An example of one MS entry procedure in DCJS [taken from 11]

Regarding cryptographic problems, the 224bit ECC (Elliptic Curve Cryptography) offers 2048bit RSA security instead of 160bits ECC which offers 1024bit RSA. So, 224bit ECC will bring a speedier computational efficiency with the same level of security, memory, and bandwidth and energy savings. Within PKM-MSH messaging, *replay attacks* are avoided using random numbers. If a message is hacked and the attackers resend the random generated number in the message it can be detected by the receiver. In doing so, the receiver ignores the message because the random number sequence doesn't match. If the random number is found, the attacker still has to verify the signature. The verification can't be completed because the attacker can not provide the private key.

VI. Conclusion

Even if WiMAX technology has complex authentication and authorization methods and very strong encryption techniques is still vulnerable on different attacks or threats. Being still a new technology, a special attention for security improvements is required in IEEE 802.16 standard. We hope that in the future they will become fewer and resolvable.

In conclusion we can say that there are and there will be ways to study security challenges for new wireless technologies until this communications will be 100% safe.

This paper wants to be an overview of most threats involved in infrastructure and IEEE 802.16 (WiMAX Technology) deployment and the security solutions needed to overcome them.

References

[1] WiMAX Forum, "Mobile WiMAX – Part I: A Technical Overview and Performance Evaluation", whitepaper, February 2006.

[2] IEEE Std 802.16™-2004 (Revision of IEEE Std 802.16-2001), "IEEE Standard for Local and Metropolitan Area Networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems", 1 October 2004.

[3] Rysavy Research and 3G Americas, "EDGE, HSPA & LTE. The Mobile Broadband Advantage", September 2008 (whitepaper).

[4] Abdelrahman Elleithy, Alaa Abuzaghleh, Abdelshakour Abuzneid, "A new mechanism to solve IEEE 802.16 authentication vulnerabilities", Computer Science and Engineering Department, Univ. of Bridgeport, CT.

[5] Mohsen Gerami, "A survey on WiMAX", IJCSIS– International Journal of Computer Science and Information Security, vol. 8, No. 2, 2010, ISSN 1947-5500, pp. 352-357.

[6] Eren, E., Detken, K., "WiMAX-Security - Assessment of the Security Mechanisms in IEEE 802.16d/e.", The 12th World Multi-Conference on Systemic, Cybernetics, and Informatics, Proceedings, Vol. III, Published by International Institute of Informatics and Systemic; 29th June/2nd July, Orlando (Florida), USA, ISBN10: 1-934272-32-7, 2008.

[7] Loutfi Nuaymi, "WiMAX: technology for broadband wireless access", John Wiley & Sons Ltd., 2007, ISBN 978-0-470-02808-7, pp. 238-238.

[8] Sen Xu, Manton Matthews, Chin-Tser Huang, "Security Issues in Privacy and Key Management Protocols of IEEE 802.16", ACM-SE 44-Proceedings of the 44th annual Southeast regional conference, ACM New York, 2006, ISBN:1-59593-315-8, pp. 113-118.

[9] Michel Barbeau, "WiMAX/802.16 Threat Analysis", Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks - Q2SWinet '05, New York, USA, ACM, October 13, 2005, ISBN: 1-59593-241-0, pp. 8-15

[10] Richard A Poisel, "Modern Communications Jamming Principles and Techniques", Artech House Inc. Publisher, ISBN 1-58053-743-x, 2004

[11] Po-Wen Chi and Chin-Laung Lei, "A prevention approach to scrambling attacks in WiMAX networks", WoWMoM'09, IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks & Workshops, 15-19 June, ISBN: 978-1-4244-4440-3, 2009, pp. 1-8.

[12] David Johnston, Jesse Walker, "Overview of IEEE 802.16 Security", Journal of IEEE Security and Privacy, IEEE Educational Activities Department Piscataway, NJ, 2(3), 2004, ISSN:1540-7993, pp. 40-48.

[13] Andreas Deininger, Shinsaku Kiyomoto, Jun Kurihara and Toshiaki Tanaka, "Security Vulnerabilities and Solutions in Mobile WiMAX", IEEE, IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.11, November 2007, pp. 7-15.

[14] Sheraz Naseer, Muhammad Younus, Attiq Ahmed, "Vulnerabilities Exposing IEEE 802.16e Networks to DoS Attacks: A Survey", Proceedings of the 9th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, SNPD2008, 6-8 August, Thailand, 2008, pp.344-349.

[15] Taeshik Shon and Wook Choi, "An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions", Proceedings of the First International Conference on Network-Based Information Systems, Springer-Verlag LNCS No.4658, September 2007, p.88.

[16] Tao Han, Ning Zhang, Kaiming Liu, Bihua Tang and Yuan'an Liu, "Analysis of mobile WiMAX security: Vulnerabilities and solutions", 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems - MASS 2008, October 2008, ISBN: 978-1-4244-2574-7, pp. 828-833.

[17] Md. Rezaul Karim Siddiqui and Sayed Mohammad Atiqur Rahman, "Security analysis of the WiMAX Technology in Wireless Mesh networks", Master thesis, Blekinge Institute of Technology, Karlskrona, Sweden, 2009, pp. 45.

[18] Trung Nguyen and Raj Jain, "A survey of WiMAX security threats", White Paper, April 2009, http://www.cse.wustl.edu/~jain/cse571-09/ftp/wimax2/index.html